A Security Scheme for Wireless Sensor Networks

Hacène Fouchal*, Javier Biesa **, Elena Romero **, Alvaro Araujo**, Octavio Nieto Taladrez**
(*) Centre de recherche CReSTIC, Université de Reims Champagne-Ardenne, France,
hacene.fouchal@univ-reims.fr
(**) Departamento de Ingeniería Electrónica, Universidad Politécnica de Madrid, Spain
jblesa@die.upm.es, elena@die.upm.es, araujo@die.upm.es, octavio.nieto-taladriz@upm.es

Abstract

Security is critical for wireless sensor networks (WSN)deployed in hostile environments since many types of attacks could reduce the trust on the global functioning of any WSN. Many solutions have been proposed to secure communications for WSNs and most of them rely on a centralized component which behaves as a certificate authority. We propose in this paper a distributed solution able to ensure authentication of nodes at any time without having any on-line access to a certificate authority. Each node will be equipped with a Trusted Platform Module (TPM) which is able to store keys with security. Each node will have its own public key and private key pair in the TPM and a certificate of the public key. The certificate is issued off-line when setting-up the node. When a node communicates with another, it has to sign the message with its own private key (done securely by the TPM) and sends the message, the signature and the certificate of the public key. The evaluation of the solution has been done using simulation and the overhead added by integrating authentication does not exceed 15% of energy consumption.

***Index Terms*—WSN, Security, TPM, authentication.**

I. Introduction

Wireless sensor networks are based on a combination of sensing function with computing and communication which opens the possibility to many applications to be developed in many areas. Securing wireless sensor networks, is particularly challenging since many constraints exist:

- Reduced memory resources: we do not have enough space to store data about all nodes.
- Their ad-hoc nature, potentially forcing sensor nodes to interact with many different networks over time.
- Sensor nodes are not tamper resistant, therefore any secrete key or code could be extracted easily.
- The use of PKI is not possible since a connection to the internet (and to an certificate authority) is not possible.

Wireless sensor nodes have to work using their limited energy capacity for sensing, computing and transmitting information in a wireless environment since recharging or replacing batteries is not always possible.

Security is critical for sensor networks deployed in hostile environments. Indeed, it is well known that wireless communication is subjected to threats such as flooding attack, denial of service attack jamming attack, selective forwarding attack. For these reasons, ensuring node authentication protects communications against these attacks. Security mechanisms deployed in WSNs should involve collaboration between all the nodes due to the decentralized nature of the nodes and the absence of any infrastructure. In addition, it is much critical when the nodes are equipped with security items as secrete keys and any other sensitive data. Intruders may deploy among

978-1-5090-1328-9/16/$31.00 ©2016 IEEE